IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

WILLIAM SCOTT COLLINS, et al.,

Plaintiffs,

v. No. CV 20-869 JCH/CG

GREY HAWK TRANSPORTATION, LLC, et al.,

Defendants.

ORDER APPOINTING INDEPENDENT FORENSIC EXPERT AND ESTABLISHING PROTOCOL FOR INSPECTION

THIS MATTER is before the Court upon the Court's *Memorandum Opinion and Order*, (Doc. 125), ordering Defendant Grey Hawk Transportation, LLC to show cause why an expert should not be appointed pursuant to Federal Rule of Evidence 706, filed August 17, 2021; Defendant Grey Hawk Transportation, LLC's *Response to the Court's Order to Show Cause*, (Doc. 127), filed August 20, 2021; the Court's *Order Setting Forensic Expert Schedule & Modifying Discovery Schedule*, (Doc. 135), filed August 31, 2021; and the telephonic hearing held on September 10, 2021.

IT IS HEREBY ORDERED that an independent forensic expert shall be **APPOINTED** pursuant to Federal Rule of Evidence 706, and that following protocol shall govern the work of the independent forensic expert and the inspection process:

1. **Nghi Tran of Digital Discovery, LLC** (the "Inspector") shall conduct the forensic inspection described herein. On or before **September 10, 2021 at 5:00 p.m.** (CST), counsel for William Scott Collins ("WSC") and Sarah Collins ("SC") shall make available to the Inspector the following devices and iCloud accounts:

   a. William Scott Collins' cell phone;

b. Sarah Collins' cell phone;

c. William Scott Collins' iCloud account;

d. William Scott Collins' iTunes account;

e. Sarah Collins' iCloud account;

f. Sarah Collins' iTunes account (collectively, the "Devices and Accounts").

2. Simultaneously with this delivery, counsel for WSC and SC shall provide all login and password information associated with the Devices and Accounts to the Inspector. If the Inspector deems additional passwords are necessary to complete the inspection (defined below), counsel for WSC and SC shall provide the additional passwords to the Inspector.

3. Within three business days following the Inspector's receipt of the Devices and Accounts, the Inspector shall perform the following tasks:

a. create a list of all original media/equipment the Inspector is inspecting;

b. create a full mirror-image of the Devices and Accounts; and

c. conduct searches on the contents of the Devices and Accounts (the "Inspection"). When extracting data from the phones, the expert shall use Cellebrite software and tools.

4. The Inspector shall retain only a single copy of the mirror-image of all Devices and Accounts inspected. The Inspector shall not release any documents or information obtained pursuant to this protocol that is contained on the Devices and Accounts or the results of the Inspection except as expressly set forth below, unless further ordered to do so by the Court. The Inspector's Inspection of the Devices and

Accounts will not waive any applicable privilege, objection, or other doctrine assuring the privacy and confidentiality of the information on the Devices and Accounts. The Inspector will maintain all information in the strictest confidence.

5. The information to be extracted from the Inspector's search of the Devices and Accounts shall include any document or file generated or created in the 24-hour period of December 21, 2018. All data, including without limitation documents, records, files, logs, deleted materials, and any other data resulting from Inspector's searches of the Devices and Accounts pursuant to Exhibit A shall be deemed the "Recovered Information."

6. Within two business days of completion of the Inspection, the Inspector shall separately provide the Parties' counsel with (1) a report detailing all tasks performed and the methodology used for performing those takes, and (2) a forensic report detailing the Recovered Information.

a. For emails, the forensic report detailing the Recovered Information shall contain, to the extent the information is available: (i) the subject line of the email; (ii) the to, from, cc, and bcc fields; (iii) the date sent and/or received; and (iv) a list of the name and type of any file attached to the email.

b. For SMS, MMS, or other applications including without limitation iMessenger or other platforms used to exchange between persons communication, pictures, and/or other data, the forensic report detailing the Recovered Information shall contain, to the extent available: the name(s) of the sender(s); the name(s) of the recipient(s);

the date of the transmission; and a generic description of the information exchanged.

c. For documents and files, the forensic report shall contain, to the extent the information is available: (i) the full name of the file including extension; (ii) the file path/directory/folder in which the file is found; (iii) file size; (iv) the file's MD5 Hash; (v) date created; (vi) date modified; (vii) date last accessed and/or deleted; and (viii) author.

d. In addition to collecting the metadata as set forth herein, the Inspector shall identify any records changed inside any databases to information generated in the 24-hour period, to include all system databases and all application databases. The Inspector shall also identify any configuration data that changed with respect to information generated in 24-hour period.

7. Within two business days of delivery of the forensic report, Plaintiffs' counsel shall provide the Inspector and Grey Hawk's counsel with a list of Recovered Information, if any, for which irrelevance or a privilege is claimed. If Plaintiffs claim irrelevance or privilege with respect to any Recovered Information, such materials shall be produced only to Plaintiffs' counsel and, within two (2) days, Plaintiffs shall produce from that set of materials any non-objectionable information to Grey Hawk's counsel and Plaintiffs' counsel shall create, and provide to Grey Hawk's counsel via email, a withholding log separately listing each item of Recovered Information for which irrelevance or privilege is claimed (the "Withholding Log"). The Withholding Log shall specify each item of Recovered Information by date, type (e.g., email, letter, etc.),

sender(s) and/or author(s), all recipients (including person copied), description without revealing the privileged content of the document, and provide an explanation of the basis for withholding such document. Grey Hawk shall have the right to challenge the withholding of any item of Recovered Information set forth on the Withholding Log.

8. All Recovered Information for which Plaintiff does not claim irrelevance or privilege shall be immediately produced to counsel for Grey Hawk.

9. All costs associated with the Inspection, the forensic report, and the production of recovered documents shall be paid by counsel for Plaintiffs.

10. The Parties agree to make all reasonable efforts to facilitate this Protocol, and to do their utmost to proceed quickly through all of these steps.

IT IS SO ORDERED.

THE HONORABLE CARMEN E. GARZA
CHIEF UNITED STATES MAGISTRATE JUDGE